Forcepoint

Descritivo

Prevenção de invasões com o firewall de próxima geração da Forcepoint

A Forcepoint oferece um dos sistemas de prevenção de invasões (IPS) mais bem avaliados do setor para proteger redes corporativas distribuídas – em data centers, escritórios, filiais e na nuvem.

As soluções de segurança de rede da Forcepoint oferecem um dos sistemas de prevenção contra invasões mais seguros do setor. Com a melhor classificação em testes independentes, o Forcepoint Next-Gen Firewall pode ser implementado como um dispositivo IPS de camada 2 autônomo ou como parte de um firewall de camada 3 de última geração com recursos completos em ambientes físicos, virtuais e em nuvem. Derrota evasões, exploits e malwares que os atacantes usam para invadir e se espalhar nas redes corporativas.

Arquitetura única para eficácia e velocidade

O Forcepoint Next-Gen Firewall usa uma abordagem dinâmica baseada em fluxo para inspeção que vai além da simples inspeção de pacotes. Reconstrói e examina as cargas úteis reais, derrotando as técnicas de evasão que camuflam exploits e malwares.

Além disso, a descriptografia granular de alta velocidade desmascara ataques que tentam se esconder no tráfego SSL/TLS. O Forcepoint analisa cada fluxo de payload, decodificando as várias camadas de protocolos para procurar configuração de protocolo, metadados e cabeçalhos anômalos ou malformados.

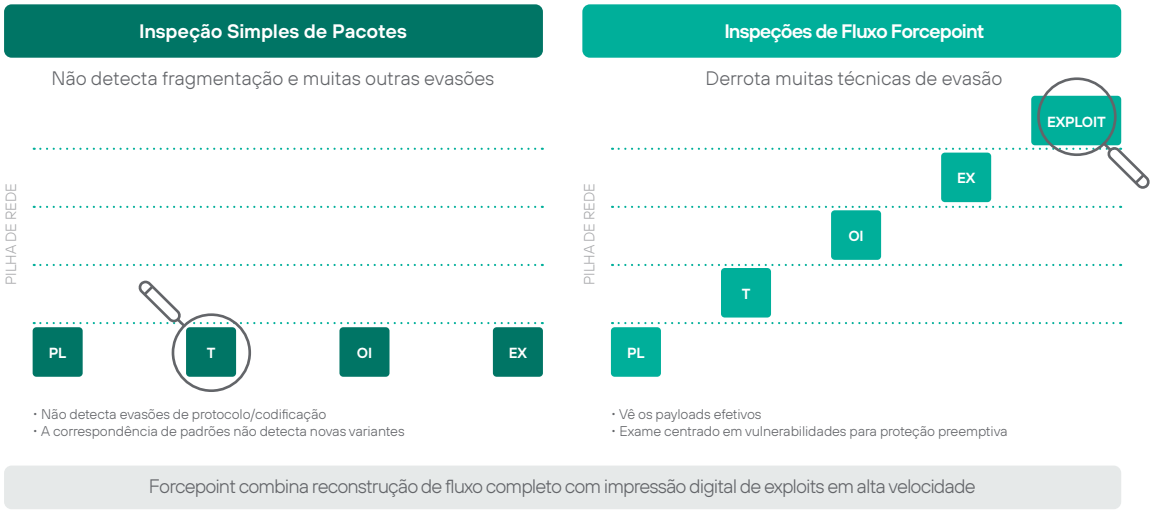
Em seguida, a Forcepoint aplica técnicas avançadas para examinar o conteúdo da transmissão em busca de sinais de exploits contra vulnerabilidades em muitos tipos de sistemas. Diferente dos mecanismos de assinatura baseados em padrões detalhados, a abordagem mais sofisticada da Forcepoint permite que esses ataques sejam identificados com uma impressão digital única e concisa. As impressões digitais são correspondidas usando autômatos finitos determinísticos de alta velocidade (DFA) adaptados a cada contexto de protocolo, permitindo que novas impressões digitais sejam incorporadas com quase nenhum impacto nos recursos da CPU.

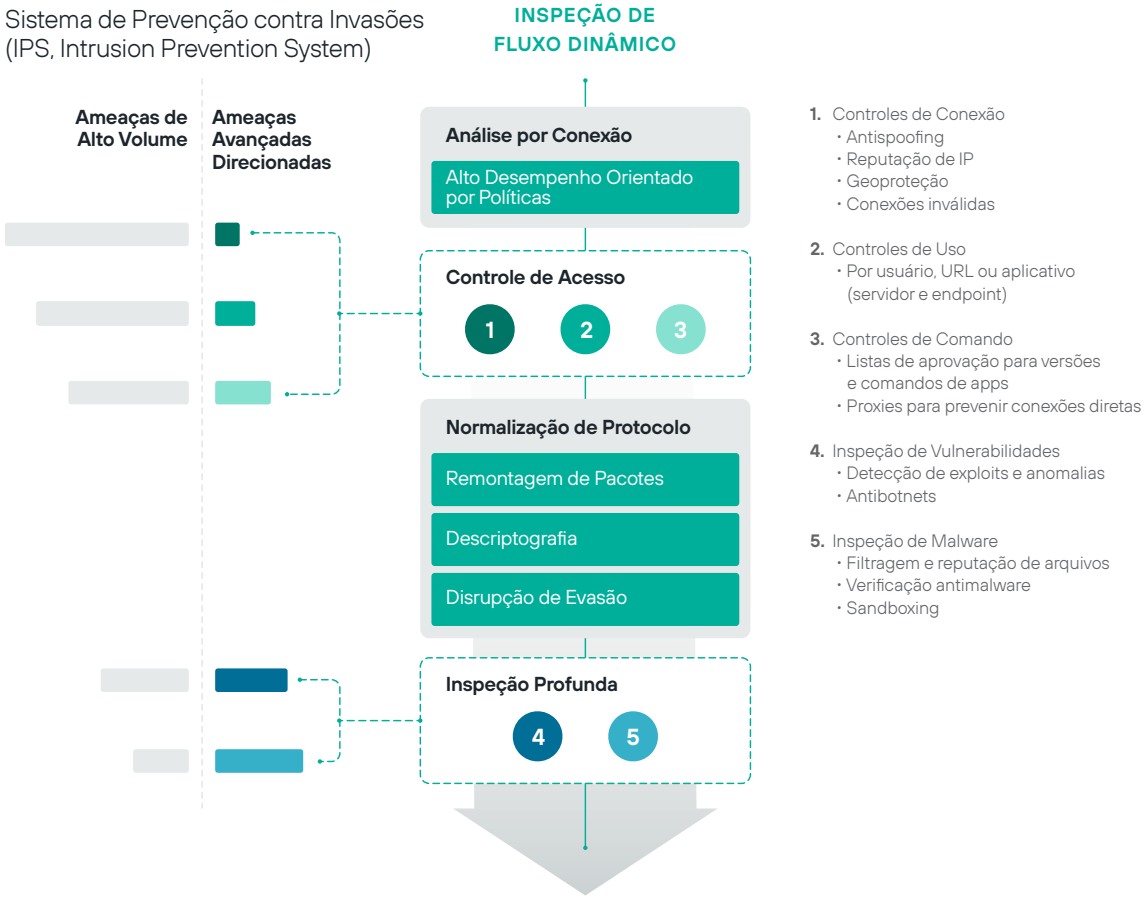
Atualizações contínuas para ficar à frente dos atacantes

A equipe de pesquisa global da Forcepoint examina constantemente os feeds de inteligência de ameaças, relatórios de vulnerabilidade de diferentes fontes e uma variedade de sistemas de teste para analisar exploits e vulnerabilidades. Novas impressões digitais são publicadas conforme necessário em nosso serviço de nuvem e são baixadas automaticamente pelos sistemas de segurança de rede Forcepoint. Com essa abordagem proativa, as equipes de TI têm tempo para analisar patches recém-publicados e implementar esforços de correção sem receio de comprometimento imediato.

Bloqueio de Dia Zero e conteúdo indesejado

Os produtos de segurança de rede da Forcepoint também fornecem várias camadas de defesa contra ataques anteriormente desconhecidos e conteúdo indesejável. Os arquivos transmitidos passam por uma rigorosa verificação de reputação e malware, e novas ameaças, como ataques de dia zero, podem ser descobertas com nossa avançada tecnologia de sandboxing. A Forcepoint é uma das pioneiras em categorização e filtragem de sites e conteúdo; com nossos dispositivos IPS e firewalls, as organizações podem cumprir com mais facilidade as regulamentações de local de trabalho, limitar a exposição de dados pessoais e impedir que os usuários acessem sites com conteúdo perigoso.





Resiliência fail-open

Os appliances da Forcepoint são compatíveis com diversas placas de rede modulares, incluindo interfaces fail-open que mantêm o tráfego funcionando mesmo se o Next-Gen Firewall perder energia.

Proteção para manter a sua organização funcionando

A cada dia, os atacantes ficam melhores em invadir redes corporativas, aplicativos, data centers e endpoints. Depois que entram, podem roubar propriedade intelectual, informações de clientes e outros dados confidenciais, causando danos irreparáveis à sua confiança e reputação.

Os ataques na Internet estão indo além da simples transmissão de exploits de vulnerabilidades. Cada vez mais, novas técnicas estão sendo usadas para evadir a detecção por dispositivos tradicionais de segurança de rede, incluindo muitos firewalls de marca.

Essas evasões funcionam em vários níveis para camuflar exploits e malwares, tornando-os invisíveis para a inspeção tradicional de pacotes baseada em assinaturas. Com as evasões, até mesmo ataques antigos que foram bloqueados por anos podem ser usados de repente para comprometer sistemas internos.

A Forcepoint usa uma abordagem diferente. Nosso mecanismo IPS líder do setor foi projetado para os três estágios de defesa de redes: derrotar evasões, detectar exploits de vulnerabilidades e bloquear malwares. Pode ser implementado de forma transparente por trás de firewalls existentes para adicionar proteção sem interrupção ou como parte de nosso Next-Gen Firewall completo para segurança completa.

Todos os produtos de segurança de rede Forcepoint são atualizados continuamente, administrados centralmente e podem compartilhar políticas e painéis de segurança de forma transparente em toda a rede. Com Forcepoint, você pode manter sua organização segura – de forma confiável, consistente e eficiente – em todos os data centers, redes de escritório, filiais ou ambientes de nuvem.

Resultados

- Menos invasões
- Mais segurança sem disrupção
- Menos exposição a novas vulnerabilidades enquanto as equipes de TI se preparam para implementar novos patches
- Implementação mais segura de filiais, nuvens ou datacenters
- Custo total de propriedade mais baixo (TCO) para infraestrutura de segurança e redes

Principais recursos

- Implementação como um IPS de camada 2, firewall de última geração de camada 2 ou como parte de um firewall de última geração de camada 3
- Sistema de Detecção de Intrusão (IDS) e Sistema de Prevenção de Intrusão (IPS) combinados para proteger e defender
- Inspeção de fluxo que examina as cargas úteis efetivas
- Pioneiro em defesas antievasão
- Descriptografia em alta velocidade com controles de privacidade granulares
- Detecção de anomalias e uso inadequado de protocolos
- Detecção de exploits e malwares com DFA em alta velocidade
- Detecção de negação de serviço (DoS)
- Defesas antibots
- Sandboxing de dia zero com appliance em nuvem ou no local
- Filtragem de URLs líder no setor
- Interfaces de rede fail-open modulares para dispositivos
- Capacidades e desempenho unificados em todas as implementações
- Administração centralizada com base em políticas
- Atualizações rápidas sem tempo de parada

Especificações do Forcepoint Next-Gen Firewall

PLATAFORMAS COM SUPORTE	
Appliances	Várias séries de appliances modulares para implementação em data centers, bordas de rede e filiais
Infraestrutura de nuvem	Amazon Web Services, Microsoft Azure
Appliance virtual	Sistemas x86 de 64 bits; ambiente virtualizado VMware ESXi, VMware NSX, Microsoft Hyper-V e KVM
Modelos de implementação	IPS autônomo (camada 2, com módulos opcionais de interface de rede fail-open), parte do NGFW (camada 3)
Contexto virtual	Virtualização para separar contextos lógicos com interfaces e políticas separadas

INSPEÇÃO	
Normalização de tráfego de várias camadas / inspeção profunda a todo vapor	› Reconstrói e analisa payloads reais para garantir a integridade dos fluxos de dados › Descarta segmentos duplicados de nível inferior que podem levar a ambiguidades quando remontados
Defesas antievasão	Bloqueia fragmentos fora de ordem, segmentos sobrepostos, manipulação de protocolos, ofuscação, truques de codificação
Detecção de contexto dinâmico	Protocolo, aplicativo, tipo de arquivo
Manipulação/ inspeção de tráfego específico do protocolo	Ethernet, H.323, GRE, IPv4, IPv6, ICMP, IP-in-IP, encapsulamento IPv6, UDP, TCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MGCP, MSRPC, NetBIOS Datagram, OPC Classic, OPC UA, Oracle SQL Net, POP3, POP3S, RSH, RSTP, SIP, SMTP, SSH, SunRPC, NBT, SCCP, SMB, SMB2, SIP, TCP Proxy, TFTP, inspeção integrada com Sidewinder Security Proxies
Descriptografia granular de tráfego SSL/TLS	› Descriptografia de alto desempenho de fluxos de cliente e servidor HTTPS › Controles orientados por políticas para proteger a privacidade dos usuários e limitar a exposição das organizações a dados pessoais › Verificações de validade do certificado TLS e lista de isenção baseada em nome de domínio do certificado
Detecção de exploits de vulnerabilidades	› Independente de protocolo, qualquer protocolo TCP/UDP com detecção e proteção contra evasão › Suporte para integrações de assinaturas Snort para personalizar e aprimorar a abordagem de segurança geral › A abordagem sofisticada de impressão digital elimina a necessidade de muitas assinaturas › O mecanismo de correspondência de autômatos finitos determinísticos de alta velocidade (DFA) administra novas impressões digitais rapidamente › Atualização contínua de impressões digitais da Forcepoint
Impressões digitais personalizadas	› Correspondência de impressões digitais independente de protocolo › Linguagem de impressão digital baseada em expressões regulares com suporte para aplicativos personalizados
Reconhecimento	Varredura TCP/UDP/ICMP, detecção furtiva e varredura lenta em IPv4 e IPv6
Antibotnets	› Detecção baseada em descriptografia e análise de sequência de comprimento de mensagem › Categorização de URLs atualizada automaticamente para bloquear ou alertar os usuários sobre sites de botnets
Correlação	Correlação local, correlação do servidor de registros
Proteção contra DoS/DDoS	› Detecção de inundação SYN/UDP com limitação de conexão simultânea, compressão de registros baseada em interface › Proteção contra métodos de solicitação HTTP lentos, limite de conexão meio aberto › Separação entre plano de controle e plano de dados
Métodos de bloqueio	Bloqueio direto, redefinição de conexão, lista de rejeição (local e distribuída), resposta HTML, redirecionamento HTTP
Registro de tráfego	Registros/trechos automáticos de tráfego em situações de uso indevido
Atualizações automáticas	› Atualizações dinâmicas contínuas por meio do Forcepoint Security Management Center (SMC) › Atualiza os patches virtuais e fornece detecção e prevenção para ameaças emergentes

Especificações do Forcepoint Next-Gen Firewall, continuação

DETECÇÃO AVANÇADA DE MALWARE E CONTROLE DE ARQUIVOS	
Protocolos	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
Filtragem de arquivos	Filtragem de arquivos baseada em políticas com processo de seleção descendente eficiente; mais de 200 tipos de arquivos suportados em 19 categorias de arquivos
Reputação de arquivos	Verificação e bloqueio de reputação de malware de alta velocidade com base na nuvem
Verificação antivírus de arquivos	Mecanismo de verificação antivírus local*
Sandboxing de dia zero	Forcepoint Advanced Malware Detection disponível para Forcepoint NGFW em nuvem, no local ou um serviço air-gapped semelhante ao usado pelo Forcepoint Web Security, Forcepoint Email Security e Forcepoint CASB

FILTRAGEM DE URLS	
Categorização de URLs	Habilitada por Forcepoint ThreatSeeker Intelligence, também usada por Forcepoint Web Security e Forcepoint Email Security
Atualizações automáticas	Atualizado continuamente à medida que novos sites são analisados
Aplicação de políticas de acesso com base em categorias	Filtragem de URLs do Forcepoint NGFW disponível como assinatura adicional

ADMINISTRAÇÃO E MONITORAMENTO	
Interfaces de administração	Sistema de administração centralizado de nível empresarial com recursos de análise de registros, monitoramento e geração de relatórios (consulte o descritivo do Forcepoint Security Management Center para obter detalhes)
Monitoramento SNMP	SNMPv1, SNMPv2c e SNMPv3
Captura de tráfego	Tcpdump do console, captura remota com Forcepoint Security Management Center
Comunicação de administração de alta segurança	Força de segurança de 256 bits na comunicação de administração de mecanismo
Certificações de segurança	Perfil de proteção de dispositivos de rede de critérios comuns com firewall de filtro de tráfego estável de pacote estendido, certificado de criptografia FIPS 140-2, CSPN por ANSSI, certificação de segurança de primeiro nível USGv6
Agente de contexto de endpoint	Listas de aprovações e rejeições de aplicativos cliente executados em hosts e dispositivos de usuários finais. Pode impedir que arquivos não confiáveis façam conexões de saída e habilita controles granulares que podem ser personalizados para atender às necessidades de sua organização.

*A verificação antimalware local não está disponível em appliances 110/115.